



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/611,775	07/07/2000	Andrew K. Krumel	802-001	6989

7590 02/27/2004

Loudermilk & Associates  
P.O. Box 3607  
Los Altos, CA 94024-0607

EXAMINER
----------

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 02/27/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/611,775

Applicant(s)

KRUMEL, ANDREW K.

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 07 July 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-66 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-38 and 40-66 is/are rejected.
- 7) ☒ Claim(s) 16 and 39 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 July 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. The IDS of 10/17/2000 (paper #2) has been received and considered.
2. Claims 1-66 are pending.

### *Claim Objections*

3. Claim 16 is objected to because of the following informalities: The claim depends upon "claim 16". *For the purposes of this office action, claim 16 is understood to depend upon claim 15.* Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1-4, 11-16, 31-38, 40 & 41 are rejected under 35 U.S.C. 102(a) as being anticipated by "Design of A High-Performance ATM Firewall" by Xu.

Regarding claim 1, Xu teaches receiving a communication packet from the external computing system/WAN over the network (page 272 §2.1), the packet having at least a first portion/header and an end portion/last cell, and transmitting/passing the packet to the internal computing system/LAN (page 277 ¶2-4), in parallel with the step of receiving and transmitting the packet, determining characteristics/class of the packet from the first portion/header (page 272 §2.1, page 277 ¶3), in parallel with the step of receiving and transmitting the packet, performing

Art Unit: 2134

a plurality of checks/TCP/IP rules on the packet (page 272 ¶1, page 275 ¶1), wherein at least certain of the plurality of checks are performing in parallel with other of the plurality of checks (page 280 ¶1-3 & page 287 ¶1), in parallel with the step of receiving and transmitting the packet, determining if the packet should be a valid/safe packet or an invalid/unsafe packet based on the plurality of checks/rules (pages 275-278 §2.2.3), and after receiving the end portion/last cell of the packet, selectively altering/passing or generating randomly the end portion of the packet based on whether the packet has been determined to be a valid/safe packet or an invalid/unsafe packet, wherein the packet is selectively altered/generated randomly to be invalid/unsafe if it was determined that the packet should be an invalid/unsafe packet (page 277 ¶2).

Regarding claim 2, Xu discloses the packet being analyzed in real time to determine if the packet should be valid or invalid while the packet is being concurrently transmitted to the internal computing system/LAN (page 277 ¶2-3).

Regarding claim 3, Xu discloses examining the packet before the last cell has arrived (page 277 ¶2-3)

Regarding claim 4, Xu discloses determining a packet invalid/unsafe if it is determined that the packet is harmful/dangerous (page 272 §2.1 & page 278 ¶2).

Regarding claim 11, Xu discloses the plurality of checks/rules being performed with a programmable logic device/ATM firewall with cache, wherein logic within the programmable logic device/ATM firewall with cache is selectively programmed to perform the plurality of checks in parallel with the receiving and transmitting of the packet (page 276 ¶2-3).

Regarding claim 12, Xu discloses a physical interface/input module receiving the packet from the network (page 284 §4.2) wherein the packet is coupled to the programmable logic

Art Unit: 2134

device/ATM firewall with cache, wherein the packet is coupled from the programmable logic device to a second physical interface/output module (page 286 §4.3) for transmission to the internal computing system/LAN (page 282 Fig. 2 & page 283 §4.1 & Fig. 3).

Regarding claim 13, Xu discloses the programmable logic device/ATM firewall with cache performing a plurality of checks while the packet is being coupled from the first physical interface/input module to the second physical interface/output module (pages 284-286 & page 277 ¶2-4).

Regarding claims 14 & 15, Xu discloses filtering based on port numbers (page 275 ¶1).

Regarding claim 16, Xu discloses filtering based on IP addresses (source and destination) (page 275 ¶1).

Regarding claim 31, Xu discloses a first interface circuit/input module for coupling data to and from an external network/WAN (page 282 Fig. 2 & page 284 §4.2), a second interface circuit/output module (page 286 §4.3 & page 283 Fig. 3) for coupling data to and from an internal network/LAN (page 282 Fig. 2 & page 283 §4.1), a programmable logic device/ATM firewall with cache coupled between the first interface circuit/input module and the second interface circuit/output module (page 282 Fig. 2 & page 283 Fig. 3), wherein as a packet is being received and transmitted between the first and second interface circuits (page 282 §2.1), the packet is simultaneously subjected to a plurality of filtering criteria/TCP/IP rules (page 272 ¶1 & page 275-278 §2.2.3) by the programmable logic device/ATM firewall with cache, wherein an end portion/last cell of the packet is selectively altered/passed or generated randomly by the programmable logic device based on the filtering criteria/rules (page 277 ¶2).

Regarding claim 32, Xu discloses the filtering criteria determining whether the packet is to be a valid/safe packet or an invalid/unsafe packet, wherein the packet is selectively altered/generated randomly to be invalid/unsafe if it was determined that the packet should be an invalid/unsafe packet (page 277 ¶2).

Regarding claim 33, Xu discloses determining characteristics/class (page 272 §2.1, page 277 ¶3), of a packet and a filter portion/call-screening service that subjects the packet to a plurality of checks/TCP/IP rules on the packet (page 272 ¶1, page 273 §2.2.1 & page 275 ¶1), while the packet is being received and transmitted between the first and second interface circuits (page 277 ¶2-3).

Regarding claim 34, Xu discloses a stateful filter portion/packet-filter (page 272 §2.1, page 273 §2.2.1, page 285 ¶2 & Fig. 5) and a non-stateful filter portion/traffic-monitor (page 272 §2.1, page 273 §2.2.1 & page 282 Fig. 2).

Regarding claim 35 & 36, Xu discloses the stateful filter portion/packet-filter subjecting the packet to one or more stateful filtering criterion/decision on current packet (page 285 ¶2) while the non-stateful filter portion/rules (page 275 ¶1) subjecting the packet to one or more non-stateful filtering criterion (page 273 §2.2.1, page 280 ¶1 & page 285 ¶2).

Regarding claim 37, Xu discloses a result aggregator logic/output module that receives one or more signals/decision from the stateful filter portion and the non-stateful filter portion (page 292 ¶1), wherein based on the received signals/decision the result aggregator logic/OM controls whether the packet is selectively altered to be invalid/dropped (page 277 ¶2 & page 292 ¶1).

Regarding claim 38, Xu discloses the result aggregator logic/OM receiving a completion signal/decision that indicates whether the stateful and/or non-stateful filter portions have subjected the packet to all of the filtering criteria (page 292 ¶3).

Regarding claim 40, Xu discloses the packet being subjected to the plurality of filtering criteria/rules (page 273 §2.2.1) in parallel with the packet being received and transmitted between the first and second interface circuits/modules (page 280 ¶1-3 & page 287 ¶1), wherein a decision is made whether to selectively alter the packet to be invalid by a time when the end portion of the packet has been received (page 277 ¶2-4).

Regarding claim 41, Xu discloses the packet being subjected to the plurality of filtering criteria in real time (page 277 ¶2-3) with the packet being received and transmitted between the first and second interface circuits/modules (page 283 Fig. 3).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 30, 44 & 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xu.

Regarding claim 44, Xu lacks basing a user-controlled switch's state (effectively enabling/disabling a predetermined portion of the filtering criteria/rules) on whether a computer coupled to the internal network is controlled to operate in a client mode or a server mode. However, official notice is hereby taken that it is known in the network firewall art/network

Art Unit: 2134

security art that a client/workstation requires different traffic needs (open ports, bandwidth, limitations on number of connections) than does a server. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to base a user-controlled switch's state on whether a computer coupled to the internal network is operating as a client or server. One of ordinary skill in the art would have been motivated to perform such a modification, as it was known in the art to do so.

Regarding claims 30 & 60, Xu lacks a speaker to provide feedback. However, official notice is hereby taken that it was known in the art, as the time the invention was made, to provide a speaker, such as a PC main board speaker, to provide audio feedback (for example on errors). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a speaker in Xu's system to provide feedback. One of ordinary skill in the art would have been motivated to perform such a modification as it was known in the art to do so.

8. Claims 5-8, 10, 17-19, 23-27, 29, 42, 43, 45, 46, 47-49, 53-57, 59, 61-63 & 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xu, as applied to claims 1 & 31 above, in view of "PacketShaper 4000 Getting Started Version 4.0" by Packeteer.

Regarding claims 5-8, 10, 42, 43, 45, 61-63 & 66, Xu discloses a firewall system and lacks detailed physical description of the device(s), and hence lacks a physical switch affecting the operation of the firewall. However, Packeteer teaches that it is known to include a power switch to enable/disable function of a device, such as an on/off switch (page 7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was



Art Unit: 2134

made to include an on/off toggle switch, thereby affecting the checks based on the state of the switch, affecting the configuration of the checking circuit (on/off), enabling/disabling the checks (on/off). The plurality of checks would selectively perform based on the state an on/off switch. An on/off switch would also control the configuration (on/off). One of ordinary skill in the art would have been motivated to perform such a modification, as it was well known in the art to do so, as taught by Packeteer (page 7).

Regarding claims 23, 24, 46, 53 & 54, Xu discloses a firewall system, as modified above, but lacks detailed physical description of the device(s), and hence lacks a reset switch. However, Packeteer teaches that it is known to include a power switch/reset switch to enable/disable/reset function of a device, such as an on/off switch (page 7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a physical reset switch/power switch to reset the device described by Xu. One of ordinary skill in the art would have been motivated to perform such a modification, as it was well known in the art to do so, as taught by Packeteer (page 7).

Regarding claims 17-19, 25, 26, 29, 47-49, 55, 56 & 59, Xu discloses a system, as modified above, but lacks visual feedback that the system is operational, the system is subject to filtering criteria, a light source indicative of the operating status having a first color or second color depending on the status and lacks an LED. However, Packeteer teaches that it is known in the art to provide a "status LED", being green or amber in color depending on whether shaping (filtering) is on/operational (page 41) on a hardware packet-shaper/packet-filter (page 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a status LED in Xu's system. One of ordinary skill in the art

would have been motivated to perform such a modification to convey status information, as was known in the art, as taught by Packeteer (pages 1 & 41).

Regarding claims 27 & 57, Xu discloses a system, as modified above, but lacks a light source that is selectively controlled to blink depending on the operating status. However, Packeteer teaches that it is known to include “network LEDs” to that flicker/blink when transmission or receiving activity occurs (page 41) in a hardware packet-shaper/packet-filter (page 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include network LEDs in Xu’s system. One of ordinary skill in the art would have been motivated to perform such a modification to convey activity information, as was known in the art, as taught by Packeteer (pages 1 & 41).

9. Claims 20-22 & 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xu in view of Packeteer, as applied to claims 18 & 47 above, in further view of “BlackICE Pro User’s Guide Version 2.0” by Network Ice Corporation (NIC). Xu discloses a system, as modified above, but lacks audio or visual feedback when the system has rejected one or more packets, when it is suspected to be under attack, or the severity of the attack. However, NIC teaches that to make users aware of attacks and spot trends and patterns of attacks, it is useful to provide a list of possible attacks on the system (page 3 Fig. 3) and indicating the severity (page 21). Further, when a critical or serious event occur, they can cause the blocking of addresses and ports/rejection of packets, and indicate this to the user (page 21 & page 37). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use visual indicators to indicate when the system has rejected packets and when the system is

Art Unit: 2134

under attack and to indicate the severity of an attack. One of ordinary skill in the art would have been motivated to perform such a modification to make users aware of attacks and to spot trends, as taught by NIC (pages 1, 3, 21 & 37).

10. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Xu, as applied to claim 7 above, in view of U.S. Patent 6,052,788 to Wesinger, Jr. et al. (Wesinger). Xu discloses a system, as modified above to include a user-controlled switch such as a power switch, but lacks the circuit being configured or reconfigured based on commands from the internal computing system/LAN. However, Wesinger that configuration of firewalls may be easily accomplished by running a "configurator" which provides a Web-based front-end for editing configuration files, preferably from a secured client (col. 9 lines 31-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to change the firewall configuration based on commands from the internal computing system/LAN/secure client (through a Web-browser interface). One of ordinary skill in the art would have been motivated to perform such a modification to easily accomplish firewall configuration, as taught by Wesinger (col. 9 lines 31-46).

11. Claims 28 & 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xu in view of Packeteer, as applied to claims 27 & 57 above, in further view of "BlackICE Pro User's Guide Version 2.0" by Network Ice Corporation (NIC) in further view of U.S. Patent 6,133,844 to Ahne et al. (Ahne). Xu discloses a system, as modified above, but lacks a light blinking at a rate indicative of a severity level of an attack. Packeteer teaches blinking LEDs indicating traffic

Art Unit: 2134

activity (pages 1 & 41). NIC teaches indicating a severity level of an attack to a user (pages 1, 3, 21 & 37). Ahne teaches that on a printing device, an LED's blink rate, *inter alia*, can be altered and the LEDs can be used to convey the operating status of the device (col. 7 lines 22-52 & col. 8 lines 20-37). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the blink rate of a light, as taught by Ahne, on Xu's firewall system, as suggested by Packeteer, to indicate the severity level of an attack, as taught by NIC. One of ordinary skill in the art would have been motivated to perform such a modification to convey operating status to a user, as taught by Ahne (col. 7 lines 22-52 & col. 8 lines 20-37).

12. Claims 64 & 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xu, as applied to claim 61 above, in view of U.S. Patent 5,905,859 to Holloway et al. (Holloway). Xu discloses user specified criteria/specifying or updating rules via firewall management service (page 281 §2.2.6), but lacks details about the specific hardware involved and therefore, lacks the configuration data transferred from configuration software via a cable attachment. However, Holloway teaches that it is common in the art of managing network devices to supply an RS232 serial port connection to change configuration parameters from a local console (col. 7 lines 11-32). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to transfer configuration parameters via a cable attachment/RS232. One of ordinary skill in the art would have been motivated to perform such a modification to enable a local console to change configuration parameters, as is known in the art to do, as taught by Holloway (col. 7 lines 11-32).

***Allowable Subject Matter***

13. Claim 39 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

14. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 39, the prior art relied upon fails to teach or suggest invalidating a packet if the decision/result is not received by the time the end portion/last cell is received.

***Conclusion***

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. IBM Technical Disclosure Bulletins NN8606320 (1986), NN950431 (1995), NA81123528 (1981), NN9704141 (1997), NN9512419 (1995), NN9502341 (1995), NN9308183 (1993), NN8606254 (1986), NN83102393 (1983) and 3com SuperStack 3 Firewall data sheet were cited for relevance in the various applications of LEDs acting as indicators, through color, blink rate, etc.
- b. "Design of a High-Performance ATM Firewall", 1998 ACM was cited as and older, less refined version of the primary reference to Xu relied upon.
- c. "High-Speed Policy-based Packet Forwarding Using Efficient Multi-dimensional Range Matching" was cited for teaching intrusion alarms for network security.

- d. "Norton Personal Firewall 2000 User's Guide" was cited for relevance in software firewall methods of displaying operating information to a user.
  - e. "A High Speed Firewall Architecture for ATM/OC-3c" was cited for teaching bit-parallelism in firewall rule/policy matching.
  - f. U.S. Patent 6,092,108 was cited for relevance in packet fragmentation in packet filtering environments.
  - g. U.S. Patent 6,335,935 was cited for teaching the dropping of packets when queues are full.
  - h. U.S. Patent 6,691,168 was cited for teaching parallel rule processing to speed up network filtering.
16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703) 305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

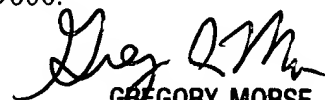
(703) 746-7239 (for formal communications intended for entry)

**Or:**

(703) 746-7240 (for informal or draft communications, please label  
"PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive,  
Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Application/Control Number: 09/611,775

Page 14

Art Unit: 2134

A handwritten signature in black ink, appearing to be 'MJS', written in a cursive style.

MJS

February 20, 2004